United States Court of Appeals
For the First Circuit

No. 02-2138

IN RE PHARMATRAK, INC. PRIVACY LITIGATION,

NOAH BLUMOFE, on behalf of himself and all others similarly situated; ROB BARRING; JIM DARBY; KAREN GRASSMAN, on behalf of herself and all others similarly situated; ROBIN MCCLARY; HARRIS PERLMAN; MARCUS SCHROERS,

Plaintiffs, Appellants,

v.

PHARMATRAK, INC.; GLOCAL COMMUNICATIONS, LTD.,

Defendants, Appellees,

PFIZER, INC.; PHARMACIA CORP.; SMITHKLINE BEECHAM PLC; GLAXO WELLCOME PLC; DOES 1-100; AMERICAN HOME PRODUCTS CORP.; NOVARTIS CORP.,

Defendants.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS
[Hon. Joseph L. Tauro, U.S. District Judge]

Before

Lynch, Circuit Judge,
Bownes, Senior Circuit Judge,
and Howard, Circuit Judge.

Adam J. Levitt with whom Daniel W. Krasner, David A.P. Brower, Wolf Haldenstein Adler Freeman & Herz LLC, Seth R. Lesser, Andrew M. Gschwind, Bernstein Litowitz Berger & Grossmann LLP, Melvyn I. Weiss, Michael M. Buchman, Dennis Stewart, William J. Doyle II, Milberg Weiss Bershad Hynes & Lerach LLP, Nancy Freeman Gans, and Moulton & Gans, P.C. were on brief for appellants.

Seymour Glanzer with whom Carmela N. Edmunds and Dickstein Shapiro Morin & Oshinsky LLP were on brief for appellees.

May 9, 2003

LYNCH, Circuit Judge. This case raises important questions about the scope of privacy protection afforded internet users under the Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2511, 2520 (2000).

In sum, pharmaceutical companies invited users to visit their websites to learn about their drugs and to obtain rebates. An enterprising company, Pharmatrak, sold a service, called "NETcompare," to these pharmaceutical companies. That service accessed information about the internet users and collected certain information meant to permit the pharmaceutical companies to do intra-industry comparisons of website traffic and usage. Most of the pharmaceutical companies were emphatic that they did not want personal or identifying data about their web site users to be collected. In connection with their contracting to use NETcompare, they sought and received assurances from Pharmatrak that such data collection would not occur. As it turned out, some such personal and identifying data was found, using easily customized search programs, on Pharmatrak's computers. Plaintiffs, on behalf of the purported class of internet users whose data Pharmatrak collected, sued both Pharmatrak and the pharmaceutical companies asserting, inter alia, that they intercepted electronic communications without consent, in violation of the ECPA.

The district court entered summary judgment for defendants on the basis that Pharmatrak's activities fell within an

exception to the statute where one party consents to an interception. The court found the client pharmaceutical companies had consented by contracting with Pharmatrak and so this protected Pharmatrak. See In re Pharmatrak, Inc. Privacy Litig., 220 F. Supp. 2d 4, 12 (D. Mass. 2002). The plaintiffs dismissed all ECPA claims as to the pharmaceutical companies. This appeal concerns only the claim that Pharmatrak violated Title I of the ECPA.

We hold that the district court incorrectly interpreted the "consent" exception to the ECPA; we also hold that Pharmatrak "intercepted" the communication under the statute. We reverse and remand for further proceedings. This does not mean that plaintiffs' case will prevail: there remain issues which should be addressed on remand, particularly as to whether defendant's conduct was intentional within the meaning of the ECPA.

I.

Pharmatrak provided its NETcompare service to pharmaceutical companies including American Home Products, Pharmacia, SmithKline Beecham, Pfizer, and Novartis from approximately June 1998 to November 2000. The pharmaceutical clients terminated their contracts with Pharmatrak shortly after this lawsuit was filed in August 2000. As a result, Pharmatrak was forced to cease its operations by December 1, 2000.

NETcompare was marketed as a tool that would allow a company to compare traffic on and usage of different parts of its

website with the same information from its competitors' websites. The key advantage of NETcompare over off-the-shelf software was its capacity to allow each client to compare its performance with that of other clients from the same industry.

NETcompare was designed to record the webpages a user viewed at clients' websites; how long the user spent on each webpage; the visitor's path through the site (including her points of entry and exit); the visitor's IP address;[1] and, for later versions, the webpage the user viewed immediately before arriving at the client's site (i.e., the "referrer URL").[2] This information-gathering was not visible to users of the pharmaceutical clients' websites. According to Wes Sonnenreich, former Chief Technology Officer of Pharmatrak, and Timothy W. Macinta, former Managing Director for Technology of Pharmatrak, NETcompare was not designed to collect any personal information whatsoever.

---

[1] An IP address is the unique address assigned to every machine on the internet. An IP address consists of four numbers separated by dots, e.g., 166.132.78.215.

[2] URLs (Uniform Resource Locators) are unique addresses indicating the location of specific documents on the Web. The webpage a user viewed immediately prior to visiting a particular website is known as the referrer URL. Search engines such as Yahoo! are common referrer URLs.

NETcompare operated as follows. A pharmaceutical client installed NETcompare by adding five to ten lines of HTML[3] code to each webpage it wished to track and configuring the pages to interface with Pharmatrak's technology. When a user visited the website of a Pharmatrak client, Pharmatrak's HTML code instructed the user's computer to contact Pharmatrak's web server and retrieve from it a tiny, invisible graphic image known as a "clear GIF" (or a "web bug"). The purpose of the clear GIF was to cause the user's computer to communicate directly with Pharmatrak's web server. When the user's computer requested the clear GIF, Pharmatrak's web servers responded by either placing or accessing a "persistent cookie" on the user's computer. On a user's first visit to a webpage monitored by NETcompare, Pharmatrak's servers would plant a cookie on the user's computer. If the user had already visited a NETcompare webpage, then Pharmatrak's servers would access the information on the existing cookie.

A cookie is a piece of information sent by a web server to a web browser that the browser software is expected to save and to send back whenever the browser makes additional requests of the server[4] (such as when the user visits additional webpages at the

---

[3] HTML is a coding language used to create documents for the Web. M. Enzer, "Glossary of Internet Terms," <http://www.matisse.net/files/glossary>.

[4] M. Enzer, "Glossary of Internet Terms," <http://www.matisse.net/files/glossary> (defining and discussing cookies). A browser, in turn, is a user's interface to the Web.

same or related sites). A persistent cookie is one that does not expire at the end of an online session. Cookies are widely used on the internet by reputable websites to promote convenience and customization. Cookies often store user preferences, login and registration information, or information related to an online "shopping cart." Cookies may also contain unique identifiers that allow a website to differentiate among users.

Each Pharmatrak cookie contained a unique alphanumeric identifier that allowed Pharmatrak to track a user as she navigated through a client's site and to identify a repeat user each time she visited clients' sites. If a person visited www.pfizer.com in June 2000 and www.pharmacia.com in July 2000, for example, then the persistent cookie on her computer would indicate to Pharmatrak that the same computer had been used to visit both sites.[5] As NETcompare tracked a user through a website, it used JavaScript and a JavaApplet to record information such as the URLs the user visited. This data was recorded on the access logs of Pharmatrak's web servers.

Pharmatrak sent monthly reports to its clients juxtaposing the data collected by NETcompare about all pharmaceutical clients.[6] These reports covered topics such as the

---

[5] Pharmatrak's cookies expired after ninety days.

[6] Pharmatrak employees supplemented the information recorded on its access logs (and sorted into databases) by conducting outside research (e.g., connecting a mid-year spike in

most heavily used parts of a particular site; which site was receiving the most hits in particular areas such as investor or media relations; and the most important links to a site.

The monthly reports did not contain any personally identifiable information about users. The only information provided by Pharmatrak to clients about their users and traffic was contained in the reports (and executive summaries thereof). Slides from a Pharmatrak marketing presentation did say the company would break data out into categories and provide "user profiles."[7] In practice, the aggregate demographic information in the reports was limited to the percentages of users from different countries; the percentages of users with different domain extensions (i.e., the percentages of users originating from for-profit, government, academic, or other not-for-profit organizations);[8] and the percentages of first-time versus repeat users. An example of a NETcompare "user profile" is: "The average Novartis visitor is a first-time visitor from the U.S., visiting from a .com domain."

---

traffic on a particular webpage with the launch of a major online advertising campaign).

[7] The NETcompare installation guide also says, "In the future, we may develop products and services which collect data that, when used in conjunction with the tracking database, could enable a direct identification of certain individual visitors."

[8] The most popular domain extensions are .com (used by for-profit entities), .edu (academic entities), .gov (government), and .org (not-for-profit).

While it was marketing NETcompare to prospective pharmaceutical clients, Pharmatrak repeatedly told them that NETcompare did not collect personally identifiable information. It said its technology could not collect personal information, and specifically provided that the information it gathered could not be used to identify particular users by name. In their affidavits and depositions, executives of Pharmatrak clients consistently said that they believed NETcompare did not collect personal information, and that they did not learn otherwise until the onset of litigation, at which point they promptly terminated the service. Some, if not all, pharmaceutical clients explicitly conditioned their purchase of NETcompare on Pharmatrak's guarantees that it would not collect users' personal information. For example, Pharmacia's April 2000 contract with Pharmatrak provided that NETcompare would not collect personally identifiable information from users. Michael Sonnenreich, Chief Executive Officer of Pharmatrak, stated unequivocally at his deposition that none of his company's clients consented to the collection of personally identifiable information.

Pharmatrak nevertheless collected some personal information on a small number of users. Pharmatrak distributed approximately 18.7 million persistent cookies through NETcompare. The number of unique cookies provides a rough estimate of the

number of users Pharmatrak monitored.[9] Plaintiffs' expert was able to develop individual profiles for just 232 users.

The following personal information was found on Pharmatrak servers: names, addresses, telephone numbers, email addresses, dates of birth, genders, insurance statuses, education levels, occupations, medical conditions, medications, and reasons for visiting the particular website.[10] Pharmatrak also occasionally recorded the subject, sender, and date of the web-based email message a user was reading immediately prior to visiting the website of a Pharmatrak client. Most of the individual profiles assembled by plaintiffs' expert contain some but not all of this information.

The personal information in 197 of the 232 user profiles was recorded due to an interaction between NETcompare and computer code written by one pharmaceutical client, Pharmacia, for one of its webpages. Starting on or before August 18, 2000 and ending sometime between December 2, 2000 and February 6, 2001, the client Pharmacia used the "get" method to transmit information from a

---

[9] Different users might have the same cookie (if, say, family members shared a computer and browser) or one user might have multiple cookies (if, for example, he used separate work and home computers to visit sites employing NETcompare, or if he revisited a NETcompare site after his first cookie expired).

[10] Plaintiffs claim in their brief that Pharmatrak also collected Social Security numbers. We are unable to tell from the record whether this is so.

rebate form on its Detrol[11] website; the webpage was subsequently modified to use the "post" method of transmission. This was the source of the personal information collected by Pharmatrak from users of the Detrol website.

Web servers use two methods to transmit information entered into online forms: the get method and the post method. The get method is generally used for short forms such as the "Search" box at Yahoo! and other online search engines. The post method is normally used for longer forms and forms soliciting private information.[12] When a server uses the get method, the information entered into the online form becomes appended to the next URL. For example, if a user enters "respiratory problems" into the query box at a search engine, and the search engine transmits this information using the get method, then the words "respiratory" and "problems" will be appended to the query string at the end of the URL of the webpage showing the search results. By contrast, if a website transmits information via the post method, then that information does not appear in the URL. Since NETcompare was designed to record the full URLs of the webpages a user viewed immediately before and during a visit to a client's site,

---

[11] Detrol is a bladder control medication.

[12] An example is the registration page at the New York Times website, which asks for a user's email address, date of birth, income, and other information.

Pharmatrak recorded personal information transmitted using the get method.

There is no evidence Pharmatrak instructed its clients not to use the get method. The detailed installation instructions Pharmatrak provided to pharmaceutical clients ignore entirely the issue of the different transmission methods.

In addition to the problem at the Detrol website, there was also another instance in which a pharmaceutical client used the get method to transmit personal information entered into an online form. The other personal information on Pharmatrak's servers was recorded as a result of software errors. These errors were a bug in a popular email program (reported in May 2001 and subsequently fixed) and an aberrant web browser.

II.

On June 28, 2001, plaintiffs filed an amended consolidated class action complaint[13] against Pharmatrak; its parent company, Glocal Communications, Ltd.; and five pharmaceutical companies: American Home Products Corp., Glaxo Wellcome, Inc.,

[13] Originally, eight lawsuits were filed in the District of Massachusetts and the Southern District of New York. The two lawsuits in the District of Massachusetts were filed on August 18, 2000. On April 18, 2001, the Judicial Panel on Multi-District Litigation issued an order transferring the six New York cases to the District of Massachusetts. The purported class, which has never been certified, consists of all persons who visited one of the defendants' websites "and who, as a result thereof, have had Pharmatrak 'cookies' placed upon their computers and have had information about them gathered by Pharmatrak."

Pfizer, Inc., Pharmacia Corp., and SmithKline Beecham Corp.[14] Plaintiffs alleged nine counts including violation of Title I of the ECPA, 18 U.S.C. § 2510 et seq.; violation of Title II of the ECPA, 18 U.S.C. 2701 et seq.; violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; violation of Mass. Gen. Laws ch. 272, § 99 (2000); violation of Mass. Gen. Laws ch. 93A (2001); invasion of privacy; trespass to chattels and conversion; and unjust enrichment.

Pharmatrak, Glocal, and a number of the pharmaceutical defendants moved for summary judgment in August 2001. In support of their motion, Pharmatrak and Glocal submitted affidavits by Macinta, Pharmatrak's former Managing Director for Technology, and Wes Sonnenreich, Pharmatrak's former CTO, as well as written descriptions of its technology and installation method and a sample monthly report delivered to pharmaceutical clients. The pharmaceutical defendants also submitted affidavits and other documents in support of their motions.

Plaintiffs argued that before summary judgment they should be allowed to conduct discovery on Pharmatrak's servers and to conduct Fed. R. Civ. P. 30(b)(6) depositions on employees of each defendant. Discovery of the servers was necessary, plaintiffs argued, to determine what information NETcompare had extracted from website users and transferred to Pharmatrak's computers. At a

[14] Glaxo Wellcome and SmithKline Beecham merged in 2000.

hearing on December 3, 2001, the court ordered discovery of the servers and Rule 30(b)(6) depositions of the defendants.[15]

The plaintiffs employed computer scientist C. Matthew Curtin and his company, Interhack, to analyze Pharmatrak's servers between December 17, 2001 and January 18, 2002. In about an hour, Curtin wrote three custom computer programs, including "getneedle.pl," to extract and organize personal information on Pharmatrak's web server access logs, which he "colloquially termed 'haystacks.'" Curtin then cross-referenced the information he extracted with other sources such as internet telephone books. Plaintiffs also conducted the Rule 30(b)(6) depositions.

After discovery was completed, Pharmatrak, Glocal, and other defendants renewed their motions for summary judgment; plaintiffs opposed these motions and moved for summary judgment against Pharmatrak and Glocal on the claim based on Title I of the ECPA.

Following a hearing on the motions, the district court issued a memorandum and order on August 13, 2002 denying plaintiffs' motion for summary judgment and granting in part defendants' summary judgment motions. In re Pharmatrak Privacy

---

[15] At the hearing, plaintiffs also sought additional documentary discovery on the ground that to date defendants had turned over only those documents that supported their defenses. In response, the court instructed both parties to "turn over . . . [a]nything that has to do with the case." The district judge added that, if defendants did not comply with this instruction, then plaintiffs should request a court order or sanctions.

Litig., 220 F. Supp. 2d at 15. The court held that the claim against Pharmatrak under Title I of the ECPA was precluded because "the Pharmaceutical Defendants consented to the placement of code for Pharmatrak's NETcompare service on their websites." Id. at 12. The court granted summary judgment to all defendants on all federal law causes of action; it then declined to retain jurisdiction over the state law causes of action and dismissed them without prejudice. Id. at 15.

III.

A. Standard of Review

This court reviews entry of summary judgment de novo. Dominguez-Cruz v. Suttle Caribe, Inc., 202 F.3d 424, 428 (1st Cir. 2000). The fact that all parties moved for summary judgment does not change the standard of review. Segrets, Inc. v. Gillman Knitwear Co., 207 F.3d 56, 61 (1st Cir. 2000). We view the record in the light most favorable to the party opposing summary judgment, indulging all reasonable inferences in that party's favor. Euromotion, Inc. v. BMW of N. Am., Inc., 136 F.3d 866, 869 (1st Cir. 1998). Summary judgment is appropriate where there is no genuine issue of material fact and the moving party is entitled to judgment as a matter of law. United Parcel Serv. v. Flores-Galarza, 318 F.3d 323, 330 (1st Cir. 2003).

We also review a district court's interpretation of a statute de novo. Bryson v. Shumway, 308 F.3d 79, 84 (1st Cir. 2002).

B. Elements of the ECPA Cause of Action

ECPA amended the Federal Wiretap Act by extending to data and electronic transmissions the same protection already afforded to oral and wire communications. 1 R.T. Nimmer, Federal Statutory Restrictions, in Information Law, ch. 8, para. 34, at 8-68 (2002). The paramount objective of the Wiretap Act is to protect effectively the privacy of communications. Gelbard v. United States, 408 U.S. 41, 48 (1972); accord United States v. Vest, 813 F.2d 477, 481 (1st Cir. 1987); see Bartnicki v. Vopper, 532 U.S. 514, 523-24 (2001).

The post-ECPA Wiretap Act provides a private right of action against one who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a); see 18 U.S.C. § 2520 (providing a private right of action). The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Id. § 2510(4). Thus, plaintiffs must show five elements to make their claim under Title I of the ECPA: that a defendant (1) intentionally (2) intercepted, endeavored to

intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device. This showing is subject to certain statutory exceptions, such as consent.

In its trial and appellate court briefs, Pharmatrak sought summary judgment on only one element of § 2511(1)(a), interception, as well as on the statutory consent exception. We address these issues below. Pharmatrak has not contested whether it used a device or obtained the contents of an electronic communication. This is appropriate. The ECPA adopts a "broad, functional" definition of an electronic communication. Brown v. Waddell, 50 F.3d 285, 289 (4th Cir. 1995). This definition includes "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photooptical system that affects interstate or foreign commerce," with certain exceptions unrelated to this case. 18 U.S.C. § 2510(12). Transmissions of completed online forms, such as the one at Pharmacia's Detrol website, to the pharmaceutical defendants constitute electronic communications. See United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 (9th Cir. 2002).

The ECPA also says that "'contents,' when used with respect to any wire, oral, or electronic communication, includes

any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). This definition encompasses personally identifiable information such as a party's name, date of birth, and medical condition. See Gelbard, 408 U.S. at 51 n.10. See generally Nix v. O'Malley, 160 F.3d 343, 346 n.3 (6th Cir. 1998) ("federal wiretap statute[] broadly define[s] 'contents'"). Finally, it is clear that Pharmatrak relied on devices such as its web servers to capture information from users.

C. Consent Exception

There is a pertinent statutory exception to § 2511(1)(a) "where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act . . . ." 18 U.S.C. § 2511(2)(d). Plaintiffs, of course, bear the burden of establishing a violation of the ECPA. Williams v. Poulos, 11 F.3d 271, 283-84 (1st Cir. 1993). Our case law is unclear as to who has the burden of showing the statutory exception for consent. United States v. Lanoue, 71 F.3d 966, 981 (1st Cir. 1995), suggests the burden is on the party seeking the benefit of the exception, here the defendant. Lanoue held that, when the defendant sought a mistrial on the grounds that the government violated § 2511(1), the prosecution had the burden to establish the statutory law enforcement exception. See also United States v. Jones, 839 F.2d 1041, 1050 (5th Cir. 1988) (when defendant in

criminal prosecution seeks to suppress intercepted communications, "the burden is on the government to prove consent" pursuant to 18 U.S.C. § 2511(2)(c)).[16] However, there is language in Poulos which could be read to say that the burden is on the party asserting a violation of the Act. 11 F.3d at 284. The issue of who has the burden to show consent was not directly addressed in Griggs-Ryan v. Smith, 904 F.2d 112 (1st Cir. 1990), an earlier case. We think, at least for the consent exception under the ECPA in civil cases, that it makes more sense to place the burden of showing consent on the party seeking the benefit of the exception, and so hold. That party is more likely to have evidence pertinent to the issue of consent. Plaintiffs do not allege that Pharmatrak acted with a criminal or tortious purpose. Therefore, the question under the exception is limited to whether the pharmaceutical defendants gave consent to the interception. Because the district court disposed of the case on the grounds that Pharmatrak's conduct fell within the consent exception, we start there.

The district court adopted Pharmatrak's argument that the only relevant inquiry is whether the pharmaceutical companies consented to use Pharmatrak's NETcompare service, regardless of how the service eventually operated. In doing so, the district court did not apply this circuit's general standards for consent under

---

[16] But cf. United States v. Phillips, 564 F.2d 32, 34 n.2 (8th Cir. 1977) (defendant in criminal prosecution bears burden of proof for statutory exceptions).

the Wiretap Act and the ECPA set forth in Griggs-Ryan, 904 F.2d 112. It also misread two district court opinions on which it purported to rely: Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153 (W.D. Wash. 2001), and In re DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

This court addressed the issue of consent under the Wiretap Act in Griggs-Ryan. A party may consent to the interception of only part of a communication or to the interception of only a subset of its communications. See Griggs-Ryan, 904 F.2d at 117-19. "Thus, 'a reviewing court must inquire into the dimensions of the consent and then ascertain whether the interception exceeded those boundaries.'" Gilday v. DuBois, 124 F.3d 277, 297 (1st Cir. 1997) (quoting Griggs-Ryan, 904 F.2d at 119). Consent may be explicit or implied, but it must be actual consent rather than constructive consent. Poulos, 11 F.3d at 281-82; see also United States v. Footman, 215 F.3d 145, 155 (1st Cir. 2000) ("The question of consent, either express or implied, may vary with the circumstances of the parties."). Pharmatrak argues that it had implied consent from the pharmaceutical companies.

Consent "should not casually be inferred." Griggs-Ryan, 904 F.2d at 117-18. "Without actual notice, consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception." Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998) (internal quotation

omitted); accord Lanoue, 71 F.3d at 981; see also Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983) ("[K]nowledge of the capability of monitoring alone cannot be considered implied consent.").

The district court made an error of law, urged on it by Pharmatrak, as to what constitutes consent. It did not apply the standards of this circuit. Moreover, DoubleClick and Avenue A do not set up a rule, contrary to the district court's reading of them, that a consent to interception can be inferred from the mere purchase of a service, regardless of circumstances. If these cases did so hold, they would be contrary to the rule of this circuit established in Griggs-Ryan. DoubleClick and Avenue A, rather, were concerned with situations in which the defendant companies' clients purchased their services for the precise purpose of creating individual user profiles in order to target those users for particular advertisements. See Avenue A, 165 F. Supp. 2d at 1156, 1161; DoubleClick, 154 F. Supp. 2d at 502, 510-11. This very purpose was announced by DoubleClick and Avenue A publicly, as well as being self-evident. See Avenue A, 165 F. Supp. 2d at 1161; DoubleClick, 154 F. Supp. 2d at 502, 510-11. These decisions found it would be unreasonable to infer that the clients had not consented merely because they might not understand precisely how the user demographics were collected. See Avenue A, 165 F. Supp. 2d at 1161-62; DoubleClick, 154 F. Supp. 2d at 510-11. The facts

in our case are the mirror image of those in DoubleClick and Avenue A: the pharmaceutical clients insisted there be no collection of personal data and the circumstances permit no reasonable inference that they did consent.

On the undisputed facts, the client pharmaceutical companies did not give the requisite consent. The pharmaceutical clients sought and received assurances from Pharmatrak that its NETcompare service did not and could not collect personally identifiable information. Further, when plaintiffs brought a suit alleging that Pharmatrak's actions meant it had not lived up to its commitment, the pharmaceutical clients promptly cancelled the service. Far from consenting to the collection of personally identifiable information, the pharmaceutical clients explicitly conditioned their purchase of NETcompare on the fact that it would not collect such information.

The interpretation urged by Pharmatrak would, we think, lead to results inconsistent with the statutory intent. It would undercut efforts by one party to a contract to require that the privacy interests of those who electronically communicate with it be protected by the other party to the contract. It also would lead to irrational results. Suppose Pharmatrak, for example, had intentionally designed its software, contrary to its representations and its clients' expectations, to redirect all possible personal information to Pharmatrak servers, which

collected and mined the data. Under the district court's approach, Pharmatrak would nevertheless be insulated against liability under the ECPA on the theory that the pharmaceutical companies had "consented" by simply buying Pharmatrak's product. Or suppose an internet service provider received a parent's consent solely to monitor a child's internet usage for attempts to access sexually explicit sites -- but the ISP installed code that monitored, recorded and cataloged all internet usage by parent and child alike. Under the theory we have rejected, the ISP would not be liable under the ECPA.

Nor did the users consent. On the undisputed facts, it is clear that the internet user did not consent to Pharmatrak's accessing his or her communication with the pharmaceutical companies. The pharmaceutical companies' websites gave no indication that use meant consent to collection of personal information by a third party. Rather, Pharmatrak's involvement was meant to be invisible to the user, and it was. Deficient notice will almost always defeat a claim of implied consent. See Poulos, 11 F.3d at 281-82; Campiti v. Walonis, 611 F.2d 387, 393-94 (1st Cir. 1979). Pharmatrak makes a frivolous argument that the internet users visiting client Pharmacia's webpage for rebates on Detrol thereby consented to Pharmatrak's intercepting their personal information. On that theory, every online communication would provide consent to interception by a third party.

D. Interception Requirement

The parties briefed to the district court the question of whether Pharmatrak had "intercepted" electronic communications. If this question could be resolved in Pharmatrak's favor, that would provide a ground for affirmance of the summary judgment. See O'Neil v. Baker, 210 F.3d 41, 46 (1st Cir. 2000). It cannot be answered in favor of Pharmatrak.

The ECPA prohibits only "interceptions" of electronic communications. "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Id. § 2510(4).

Before enactment of the ECPA, some courts had narrowed the Wiretap Act's definition of interception to include only acquisitions of a communication contemporaneous with transmission. See, e.g., Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 460-61 (5th Cir. 1994) (applying pre-ECPA interpretation to post-ECPA case). There was a resulting debate about whether the ECPA should be similarly restricted. The debate is well described in Konop, 302 F.3d at 876-79 & n.6. Other circuits have invoked the contemporaneous, or "real-time," requirement to exclude acquisitions apparently made a substantial amount of time after material was put into electronic storage. Steiger, 318 F.3d at 1048-50 (pornographic images gradually collected on hard drive);

Konop, 302 F.3d at 872-73 (static website content available on an ongoing basis); Steve Jackson Games, 36 F.3d at 458 (accumulation of unread emails). These circuits have distinguished between materials acquired in transit, which are interceptions, and those acquired from storage, which purportedly are not. See, e.g., Konop, 302 F.3d at 878.

We share the concern of the Ninth and Eleventh Circuits about the judicial interpretation of a statute written prior to the widespread usage of the internet and the World Wide Web in a case involving purported interceptions of online communications. See Steiger, 318 F.3d at 1047 (quoting Konop, 302 F.3d at 874). In particular, the storage-transit dichotomy adopted by earlier courts may be less than apt to address current problems. As one court recently observed, "[T]echnology has, to some extent, overtaken language. Traveling the internet, electronic communications are often -- perhaps constantly -- both 'in transit' and 'in storage' simultaneously, a linguistic but not a technological paradox." United States v. Councilman, 245 F. Supp. 2d 319, 321 (D. Mass. 2003).

The facts here do not require us to enter the debate over the existence of a real-time requirement. The acquisition by Pharmatrak was contemporaneous with the transmission by the internet users to the pharmaceutical companies. Both Curtin, the plaintiffs' expert, and Wes Sonnenreich, Pharmatrak's former CTO,

observed that users communicated simultaneously with the pharmaceutical client's web server and with Pharmatrak's web server. After the user's personal information was transmitted using the get method, both the pharmaceutical client's server and Pharmatrak's server contributed content for the succeeding webpage; as both Curtin and Wes Sonnenreich acknowledged, Pharmatrak's content (the clear GIF that enabled the interception) sometimes arrived before the content delivered by the pharmaceutical clients.

Even those courts that narrowly read "interception" would find that Pharmatrak's acquisition was an interception. For example, Steiger observes:

> [U]nder the narrow reading of the Wiretap Act we adopt . . . , very few seizures of electronic communications from computers will constitute 'interceptions.' . . . 'Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of [the Wiretap Act] is virtually impossible.'

318 F.3d at 1050 (paragraphing omitted) (quoting J.J. White, Email @Work.com: Employer Monitoring of Employee E-Mail, 48 Ala. L. Rev. 1079, 1083 (1997)). NETcompare was effectively an automatic routing program. It was code that automatically duplicated part of the communication between a user and a pharmaceutical client and sent this information to a third party (Pharmatrak).

Pharmatrak argues that there was no interception because "there were always two separate communications: one between the Web

user and the Pharmaceutical Client, and the other between the Web user and Pharmatrak." This argument fails for two reasons. First, as a matter of law, even the circuits adopting a narrow reading of the Wiretap Act merely require that the acquisition occur at the same time as the transmission; they do not require that the acquisition somehow constitute the same communication as the transmission. Second, Pharmatrak acquired the same URL query string (sometimes containing personal information) exchanged as part of the communication between the pharmaceutical client and the user. Separate, but simultaneous and identical, communications satisfy even the strictest real-time requirement.

E. Intent Requirement

At oral argument this court questioned the parties about whether the "intent" requirement under § 2511(a)(1) had been met.

We remand this issue because it was not squarely addressed by both parties before the district court. When Pharmatrak moved for summary judgment, it did not do so on the grounds that the statutory requirement of intent was unmet. At most, it raised the issue in passing at the hearing on the cross-motions for summary judgment.

Plaintiffs, in their motion for summary judgment, did raise the issue and argued that any interception was intentional; but the district court neither granted the motion nor addressed the issue. In its opposition to plaintiffs' motion, Pharmatrak relied

on its own motion for summary judgment, and so did not address intent. The issue has not been briefed to us.

While it is true that we can affirm the grant of summary judgment on any ground presented by the record, we will usually do so only when the issue has been fairly presented to the trial court. See Pure Distribs., Inc. v. Baker, 285 F.3d 150, 156 (1st Cir. 2002). Here it was not, and we are reluctant to determine ourselves whether there was adequate opportunity for discovery on this issue and whether there are material facts in dispute, and to resolve an issue without briefing.

Still, we wish to avoid uncertainty about the legal standard for intent under the ECPA on remand, and so we address that point. Congress amended 18 U.S.C. § 2511 in 1986 to change the state of mind requirement from "willful" to "intentional". Since "intentional" itself may have different glosses put on it,[17] we refer to the legislative history, which states:

> As used in the Electronic Communications Privacy Act, the term "intentional" is narrower than the dictionary definition of "intentional." "Intentional" means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective. An "intentional" state of mind means that one's state of mind is intentional as to one's conduct or the result of one's conduct if such conduct or result is one's conscious objective. The intentional state of mind is applicable only to conduct and results. Since one has no

[17] For example, see the distinction between general intent and specific intent described in United States v. Whiffen, 121 F.3d 18, 20-21 (1st Cir. 1997).

> control over the existence of circumstances, one cannot "intend" them.

S. Rep. No. 99-541, at 23 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3577. Congress made clear that the purpose of the amendment was to underscore that inadvertent interceptions are not a basis for criminal or civil liability under the ECPA. Id. An act is not intentional if it is the product of inadvertence or mistake. Sanders v. Robert Bosch Corp., 38 F.3d 736, 742-43 (4th Cir. 1994); United States v. Townsend, 987 F.2d 927, 930 (2d Cir. 1993). There is also authority suggesting that liability for intentionally engaging in prohibited conduct does not turn on an assessment of the merit of a party's motive. See Abraham v. County of Greenville, 237 F.3d 386, 391-92 (4th Cir. 2001) (jury instruction saying "defendant's motive is not relevant" to determination of intent under § 2511 was proper). That is not to say motive is entirely irrelevant in assessing intent. An interception may be more likely to be intentional when it serves a party's self-interest to engage in such conduct.

F. Conclusion

We **reverse** and **remand** for further proceedings consistent with this opinion.